Forensic implications of using the FireWire memory exploit with Microsoft Windows XP

A. Woodward[1] **and P. Hannay**[1]
[1]School of Computer and Information Science, Edith Cowan University, Perth, Western Australia, Australia

Abstract – *This paper examined the forensic implications of using the FireWire direct memory access function with Windows XP. If a direct connection can be made to a computer running Windows XP, then the password can be bypassed and direct access to files on the computer can be gained. It was found that EFS protected files could not be viewed after running the tool. In addition, a console can be opened with high level privileges to run other commands. The tool used for this procedure also allows for a memory dump to be taken. Circumventing passwords is of benefit to forensic investigators as it saves time. The memory dump has potential to reveal keys or other passwords that may protect encrypted data. There may be issues in terms of admissibility of any information gained using the memory dump as there is no effective way to hash the memory.*

Keywords: FireWire, IEEE 1394, Windows XP, digital forensics

1 Introduction

The FireWire memory access tool used in this work is not new. It was announced at RuxCon 2006 by Boileau [1], which built on the work of Dornseif, presented at PacSec in 2004 [2]. The initial work by Dornseif showed that direct memory access for both Linux and Apple Macintosh operating systems was possible if you could connect to the FireWire port. This code was modified by Boileau which then allowed it to be used to unlock a computer Windows XP. Whilst the forensic implications of this vulnerability were briefly considered by Dornseif [2], the full usefulness and possibilities for use by digital forensic practitioners has not.

The tool itself has several modes of operation, the most relevant to this investigation being the ability to bypass a windows password. The tool also allows for the running of a command prompt without having to log on to the computer, and also to perform a memory dump.

This type of attack is possible because the FireWire protocol, IEEE 1394 [3] is designed to be an expansion bus device. An expansion bus is designed to allow for additional functionality to be added to a computer with effectively full access to on-board RAM and CPU, as would any motherboard component. As part of the requirement of an expansion bus, and in particular the FireWire protocol itself, direct memory access is required [3]. Whilst this allows for devices connected using this method to transfer data at high speed, it is also the reason as to why the password unlock tool is able to function.

There are many methods by which information can be protected using either a password or some form of encryption to protect, or hide, depending on the situation, information from others. There are two levels of protection built in to the Microsoft Windows XP operating system to protect information. At a basic level, an account on a Microsoft Windows XP computer can be protected using a password. This can be set for a computer which is standalone, or part of a domain. To further increase the security of data stored on a hard drive, Microsoft Windows contains built in encryption which can also be used, called encrypting file system, or EFS [4]. This allows for a user to encrypt files or folders on a hard drive, and to prevent other users from being able to do so. The process is transparent once it is switched on, and provides a high level of security for data so long as the account is locked when not in use. There are some versions of Microsoft's latest operating system, Windows Vista, contain whole of disk encryption system known as BitLocker [5].

There are also third party applications available to protect data such as TrueCrypt which creates a virtual encrypted disk, which can be mounted as though it were an actual disk [6]. This program also contains two additional features which effectively hide the encrypted volume, making it both hard to detect and decrypt. Another utility which provides similar functionality is FineCrypt [7]. This tool also provides the ability to encrypt files, directories and trees. Given that the software uses 256 bit AES encryption, brute force is not really a viable option [8].

While the above tools were created with a view to protecting legitimate information at rest on a computer, these tools are also available to those who wish to use it to cover up traces of illegal activity. This creates an issue for law enforcement as they cannot view files on a suspect machine if they have been protected using either a password or some form of encryption.

There are several methods available to circumvent these protective measures. These include brute force password crackers such as John the Ripper [9], password reset utilities such as chntpw [10] and even self booting CDs with a collection of security tools such as BackTrack [11]. Most of these tools focus on the passwords used to protect the information, rather than targeting the encryption systems themselves. This is because the password is usually the weakest link, and the Windows local passwords are relatively easy to reset as they are stored in the registry. An interesting dichotomy is that that while most of these tools are developed by Blackhats and hackers, they are being increasingly used by law enforcement in order to access information on suspect computers.

This research examined the effectiveness of the FireWire memory tool against a range of parameters to determine the extent of its usefulness as a forensic unlock tool. Factors to be examined included whether the target computer was a member of a Windows workgroup, or whether it was a member of an Active Directory domain. Another factor to be examined was whether the tool would allow for the viewing of files protected with EFS on the target machine. Also of interest was the 'mode 4' of operation which in addition to unlocking the target computer also allows a command prompt to be run.

2 Methodology

The main aim of this research was to establish whether the tool worked as stated by the author. To this end, the following computer setup was used:

Attacker: IBM Intellistation 3.4GHz Pentium 4 CPU, 2GB RAM, onboard FireWire card. Debian Linux

Target: IBM S50 desktop PC 3.0GHz, 1GB RAM, Microsoft Windows XP (SP2), PCI FireWire card.

The efficacy of the tool was tested in several ways. Firstly, its ability to obtain access to a computer that had been switched off: referred to in this paper as cold boot. Secondly, was the ability to unlock a password protected, locked workstation. The tool was tested for both local and domain accounts for these scenarios. Thirdly, the ability to examine or view EFS protected files and folders were examined using both a locked workstation and a cold boot situation for both local and domain accounts.

Various other behaviours of interest and relevance to the topic were observed as part of the testing process and are also reported here.

3 Results

There were a number of parameters tested to determine the extent to which various security measures could be bypassed using the FireWire memory tool.

3.1 Password bypass

The first test was to determine the efficacy of the tool to circumvent the password logon for a computer that was a member of a workstation can be found in Table 1.

Table 1 – Efficacy of the FireWire Windows XP unlock tool against a computer that was a member of a Windows workgroup.

Tool attack mode	**Workstation Locked**	**"Cold Boot" logon**
Unlock	Yes	Yes
Unlock with command prompt	Yes	Yes

The next tests conducted were to determine whether the tool would unlock a computer that was a member of an Active Directory domain (Table 2).

Table 2 - Efficacy of the FireWire Windows XP unlock tool against a computer that was a member of an Active Directory Domain.

Tool attack mode	**Workstation Locked**	**"Cold Boot" logon**
Unlock	Yes	No
Unlock with command prompt	Yes	No

3.2 EFS

Files protected by EFS could be accessed but only under a finite set of circumstances. Effectively, access to EFS protected files was only possible if the legitimate user had already viewed the file and locked the workstation. Rebooting the workstation or logging off removed the ability to view EFS protected files.

Bypassing the Windows login from cold boot provided access to the underlying file system, but did not allow access to files protected with EFS.

A folder protected with EFS could be viewed, and the contents of the folder also viewed, but as pointed out previously, EFS protected files could not be viewed, unless they had previously been viewed by the legitimate user.

3.3 Other observations

Once the computer has been unlocked using the tool, the ability to log in without a password was still existent even after a legitimate log off and log on.

The stated aim of mode four of the tool is to allow for a command prompt to be opened on the target system. This was found to be the case, and further investigation showed that an alternate desktop could be run from this command prompt. Further to this, the task manager showed that this tool was running with system privileges, a level of access higher than that granted to an administrator.

4 Discussion

The FireWire tool was found to be successful in a number of scenarios against a password protected computer running Windows XP. It allows for a number of different attacks to be made against a computer, including bypassing the windows logon password, running a high privilege command prompt without logging in, and also performing a memory dump. The attack itself is reasonably trivial, and some modification of the code was necessary to get it to run on our test equipment, but once running, it takes only a few seconds to unlock a locked workstation.

From an initial perspective, particularly for law enforcement, the password bypass facility is of great benefit. Currently, if a computer seized by Police for investigation has password protection, then the password must be cracked, or the owner of the computer compelled to reveal the password. The former can be very time consuming with no guarantee of success, and in some instances, that time delay may be critical. There has been legislation introduced in Western Australia, specifically, S. 711AA of the *Criminal Code* (WA), whereby failing to reveal a password will result in a jail term of up to 5 years in addition to financial penalties. Again, this may also result in a significant time delay until the storage device can be analysed.

4.1 Password unlock: local vs domain accounts

The reason for the tool working for local accounts and for locked domain accounts, but not for domain cold boot logins is due to the storage location of the password. Local accounts are stored in the security accounts manager (SAM) hive, and are loaded into memory, meaning that the tool can access them. Domain accounts are stored centrally in Active Directory (AD) on a Windows server. However, once a user has logged onto a computer that is a member of a domain, the password for that account is cached locally in the following registry key:

HKEY_LOCAL_MACHINE\SECURITY\CACHE\ NL$1 through to NL$10

This allows the FireWire tool to access and bypass the password once it has been cached. This facility exists so that a user can still log on to a computer in the event that the centralized authentication server, Active Directory is not available. Specifically, a hash of the verified password is stored, not the actual username and password itself [12]. This means that whilst the password can be bypassed using the tool, a password crack utility, such as John the Ripper [9] must be run on the cached password in order to derive the password. There are both tools and instructions available in order to carry out such an attack against a cached domain password [13]. If the password can be derived, then it can be used to access an EFS protected file or folder.

4.2 chntpw vs FireWire tool to unlock

While the FireWire tool was found to be effective at gaining access to a locked or password protected workstation, there are other tools available that can be used for this purpose. Specifically, the chntpw utility is designed to quickly and easily reset the passwords for any local user account on a computer. The chntpw utility requires local access to the machine, meaning that the boot order in the BIOS needs to be changed to boot form whatever media the utility is being run from. The accounts present on the machine are presented to the user, and they can be changed to whatever password the user requires. However, there are implications for EFS protected files and folders. If the utility is used to reset the password for an account which was used to encrypt a file or folder, then access to that file or folder is lost as the password is used to create the encryption key [10].

While the chntpw utility is an appropriate tool for the offline analysis of a computer, it may not always be the best option as it can potentially destroy evidence where files or folders are encrypted with EFS. The FireWire password tool does have the limitation that the target computer must have a FireWire interface, but it does not write to the hard drive, and can allow rapid access to the data. The biggest advantage that the FireWire tool has over chntpw is that it can allow access to protected EFS files and folders under certain conditions, which chntpw cannot provide, as its use changes the key used to encrypt the files.

Effectively, choice of tool would depend on what the aim of the investigator was. If it is simply to bypass a password protected Windows computer, then chntpw would be the best option. Where access was needed to a password protected computer where EFS being used in a live environment, then the FireWire tool would be useful. However, as pointed out earlier, it only works on a locked computer, so its use for this purpose would be fairly limited.

4.3 Memory dump mode

While it would appear that the password bypass is probably the most useful of these attack modes, the memory dump has greater implications for digital forensics. If the target computer is using some form of cryptography, then it may be possible to retrieve the keys from memory. There has been other research which has looked at this process, the most recent and popularized being the co called 'cold boot' attack [14]. In this attack, the physical memory modules are literally frozen and then dumped using a memory dump is then analysed to extract any cryptographic keys that may be resident. In this case, the researchers claim to be able to extract Windows BitLocker keys from memory. BitLocker is Microsoft technology incorporated into Windows Vista that provides whole of disk encryption.

4.4 Other uses for the password unlock feature

Laptop theft is of major concern for both individuals and business. For an individual, it represents the loss of a personal asset that they may not be able to replace easily, if at all. For a government agency or a corporation, it can represent much more: the loss of corporate IP or trade secrets. There are numerous statistics which attest to the fact that laptop theft is an on-going problem. Costs of laptop theft have two components: the hardware and the claimed value of the data on the stolen device. The most recent Australian report on computer crime, produced by AUSCERT, the 2006 Australian computer crime and Security survey, indicated that of those organisations surveyed, 58% reported theft of a laptop [15].

During the course of their investigations, a large number of laptops are recovered by Police. However, most of these laptops are erased and sent to auction, as there are not sufficient resources to enable identification of the legitimate owner. The volume of recovered laptops far exceeds the amount of staff available, meaning that unless the laptop can easily be accessed in order to identify the owner in terms of the information contained within it, then no further identification is attempted. This lack identification of recovered laptops creates two problems. The first is in the increased cost to both businesses and to consumers in terms of a rise in insurance premiums. Whilst a number of these devices are found, if their legitimate owners are not able to be found, then effectively, the device at least in the eyes of insurance companies has not been recovered. The second problem has two aspects to it. The problem itself is in relation to the information contained on the laptop. If the device is not returned to the original owner then they have effectively lost all of the information on it. The other issue is that if the original owner cannot be identified, then the hard drive will be erased, and the information contained on it is again lost.

The FireWire tool could be very useful here in order to login to the computer and obtain information about the rightful owner. It could be installed on a purpose built small computer or laptop with a FireWire interface, and easily connected to recovered laptop. The advantage here over chntpw is clear, as resetting the password to gain access could potentially destroy files on the computer if EFS is being used.

5 Conclusion

This paper has demonstrated that the FireWire exploit tool has the potential to be used by forensic investigators. The main advantage of using such a tool would be to allow digital forensic practitioners to bypass the logon password, potentially saving hours or days of time cracking a password which could otherwise be used for investigation. Whilst its primary use would be to circumvent password protection, there are a number of other uses it could be put to, such as identification of stolen laptops, and viewing of EFS protected files.

Future research will examine whether the tool can be adapted to work with Microsoft Windows Vista. There is anecdotal evidence that this is the case, but no code has as yet been released to allow the authors to verify that this is the case. Another aspect that would need to be investigated is the possibility of locating cryptographic keys for other encryption or security programs that may be protecting files or folders on the hard drive.

6 References

[1] Adam Boileau, "Hit by a bus : Physical access attacks with FireWire", 2006. [Online]. Available: http://www.ruxcon.org.au/2006-presentations.shtml#14 [Accessed May 12, 2008]

[2] Maximillian Dornseif, "FireWire - all your memory are belong to us", 2004. [Online]. Available: http://md.hudora.de/presentations/firewire/PacSec2004.pdf [Accessed May 12, 2008]

[3] IEEE (1996). IEEE standard for a high speed serial bus. New York, USA: The Institute of Electrical And Electronics Engineers, Inc.

[4] Microsoft Technet, "Protecting Data by Using EFS to Encrypt Hard Drives", 2008. [Online]. Available: http://www.microsoft.com/technet/security/smallbusiness/topics/Cryptographyetc/protect_data_efs.mspx [Accessed May 13, 2008]

[5] Microsoft Technet, "BitLocker drive encryption", 2008. [Online]. Available: http://technet.microsoft.com/en-us/windows/aa905065.aspx [Accessed May 13, 208]

[6] TrueCrypt, "Free open source disk encryption", 2008. [Online]. Available: http://www.truecrypt.org/ [Accessed May 13 2008]

[7] FineCrypt, "FineCrypt – Professional encryption tool", 2008. [Online]. Available: http://www.finecrypt.net/index.htm [Accessed May 13, 2008]

[8] J. Siegfried, C. Siedsma, B-J Countryman & C.D. Hosmer, "Examining the encryption threat", International Journal of Digital Evidence, Winter 2004, Vol 2, Issue 3

[9] Openwall, "John the Ripper password cracker", n.d. [Online]. Available: http://www.openwall.com/john/ [Accessed May 13, 2008)

[10] Nordhal, P. "Office NT password and Registry Editor" Change nt password", 2008. [Online]. Available http://home.eunet.no/pnordahl/ntpasswd/ [Accessed May 20, 2008]

[11] Remote-Exploit, "BackTrack", 2008. [Online]. Available: http://www.remote-exploit.org/backtrack.html [Accessed May 13, 2008]

[12] Microsoft Help and Support, "Cached credentials security in Windows Server 2003, in Windows XP, and in Windows 2000", 2008. [Online]. Available: http://support.microsoft.com/kb/913485/en-us [Accessed May 18, 2008]

[13] Irongeek, "Cracking Cached Domain/Active Directory Passwords on Windows XP/2000/2003", 2006, March. [Online]. Available: http://www.irongeek.com/i.php?page=security/cachecrack [Accessed May 18, 2008]

[14] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest We Remember: Cold Boot Attacks on Encryption Keys", 2008. [Online]. Available: http://citp.princeton.edu/pub/coldboot.pdf [Accessed May 20, 2008]

[15] AUSCERT, "2006 Australian computer crime and Security survey", 2006. [Online]. Available: http://www.auscert.org.au/images/ACCSS2006.pdf [Accessed May 20, 2008]